AMENDMENT

In The Claims:

The claims of the application have been amended as shown in the following marked copies of the claims which replace all prior versions thereof.

1-22 (cancelled).

23. (new) A computer-implemented method of authenticating an individual's identity in real time based on a biometric signal, comprising:

receiving a biometric signal from the individual;

receiving input data representing biometric information of a known classification;

processing the input data to generate an output representing class-specific probability distributions based on the received input data;

computing a transform based on the output; and

transforming the probability distributions onto a normalized scale based on the transform, the scale having a range of values indicative of the authentic or spurious nature of the biometric signal of the individual and from which the identity of the individual is authenticated.

24. (new) The method according to claim 23, further comprising selecting at least one decision criterion based on at least one value on the normalized scale from which the identity of the individual is authenticated.

25. (new) The method according to claim 23, wherein the step of transforming comprises:

defining at least two regions of the output; and

mapping the at least two regions onto the normalized scale.

26. (new) The method according to claim 25, wherein the values of the normalized scale range from 0 to 100.

27. (new) The method according to claim 25, wherein the mapping is performed through linear interpolation.

28. (new) The method according to claim 25, wherein the at least two regions comprise varying degrees of authenticity.

29. (new) The method of claim 23, wherein the input data further comprises at least one optional transform parameter.

30. (new) The method of claim 23, wherein the normalized scale is linear in cumulative probability.

31. (new) The method of claim 23, wherein the normalized scale is derived from a ratio based on the probability distributions.

32. (new) The method of claim 23, wherein the biometric information is derived from a characteristic of an iris.

33. (new) The method of claim 23, wherein the biometric information is derived from a characteristic of speech.

34. (new) The method of claim 23, wherein the biometric information is derived from a characteristic of a fingerprint.

35. (new) A pattern recognition system adapted to authenticate an individual's identity in real time based on a biometric signal, the pattern recognition system comprising:

a computer readable medium having computer readable program code embodied thereon, the computer readable program code, when executed, implementing on the computer a method of receiving the biometric signal from the individual, receiving input data representing biometric information of a known classification, generating an output representing class-specific probability distributions based on the received input data, computing a transform based on the output, and transforming the probability distributions onto a normalized scale based on the transform wherein the scale has a range of values indicative of the authentic or spurious nature of the biometric signal of the individual and from which the identity of the individual is authenticated.

36. (new) The system of claim 35, further comprising decision criteria selection means for selecting at least one decision criterion based on at least one value on the normalized scale from which the identity of the individual is authenticated.

37. (new) The system of claim 35, wherein the transformer constructor comprises means for combining the class-specific probability distributions.

38. (new) The system of claim 35, wherein the transformer comprises:

means for defining at least two regions of the combined class-specific probability distributions; and

means for mapping the at least two regions onto the normalized scale.

39. (new) The system of claim 35, wherein the values of the normalized scale range from 0 to 100.

40. (new) The system of claim 35, wherein the transformer constructor is further adapted to receive input in the form of at least one optional transform parameter.

41. (new) The system of claim 35, wherein the at least two regions represent varying degrees of authenticity.

42. (new) The system of claim 35, wherein the normalized scale is linear in cumulative probability.

43. (new) The system of claim 35, wherein the normalized scale is derived from a ratio based on the probability distributions.

44. (new) The system of claim 35, wherein the at least one decision criterion defines a single threshold number from which to determine whether the biometric signal of the individual is authentic or spurious.

45. (new) The method of claim 35, wherein the biometric information is derived from a characteristic of an iris.

46. (new) The method of claim 35, wherein the biometric information is derived from a characteristic of speech.

47. (new) The method of claim 35, wherein the biometric information is derived from a characteristic of a fingerprint.

48. (new) A computer-implemented method of classifying an unclassified biometric signal as authentic or spurious in real time, comprising:

receiving input data representing biometric information of a known classification;

processing the input data to generate an output representing class-specific probability distributions based on the received input data;

computing a transform based on the output; and

transforming the probability distributions onto a normalized scale based on the transform, the scale having a range of values indicative of the authentic or spurious nature of the unclassified biometric signal and from which the unclassified biometric signal is classified as authentic or spurious.

49. (new) The method according to claim 48, further comprising selecting at least one decision criterion based on at least one value on the normalized scale from which the biometric signal is classified as authentic or spurious.